DocuSign Envelope ID: 15855DB6-50B5-4FA8-94EA-93EC0093760A

IT Security Procedural Guide: Identification and Authentication (IA) CIO-IT Security-01-01

Revision 7

September 21, 2022

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Revision 1 – June 23, 2005		
1	Scott/Heard	Changes made throughout the document to reflect FISMA, NIST and GSA CIO P 2100.1 requirements.	Updated to reflect and implement various FISMA, NIST and GSA CIO P 2100.1 requirements.	Various
2	Scott/Heard	Changes throughout the document to correspond with revisions made to CIO-IT Security-01-09, CIO-IT Security-01-03 and CIO-IT Security 01-04.	Updated to reflect the correlation of the CIO-IT Security Guides; and to further express policy within them as stand-alone documents.	Various
		Revision 2 – January 08, 2008		
1	Berlas	Changes made throughout the document to reflect FDCC password requirements.	OMB Memorandum M-07-11 mandates the implementation of FDCC configuration requirements.	Various
		Revision 3 – June 22, 2010		
1	Berlas/Cook	Changes made throughout the document to reflect updates in governing policy and procedures, including, NIST SP 800-53 rev3, HSPD-12, OMB e-Authentication, and FDCC password requirements.	Updated to reflect and implement OMB, NIST, and GSA CIO P 2100.1 requirements.	Various
		Revision 4 – April 17, 2015		
1	Graham	Changes to the Revision number and date of the document. Updated Cover Page, Sections 1.2, 2-4, and Appendices to reflect CIO 2100.1 and GSA guidance.	Updated to reflect and implement OMB, NIST, and GSA CIO P 2100.1 requirements	Various
2	Heard	Included references from the IT security Program Plan.	Various	Various
		Revision 5 – May 5, 2017		
1	Feliksa/ Dean/ Klemens	Changes made throughout the document to align with current OMB, NIST, and GSA policies.	Updated to align with the current version of GSA CIO 2100.1, format to latest guide structure and style, revise guidance to current GSA policies and processes.	Throughout
		Revision 6 – March 20, 2019		
1	Dean/ Klemens	Updated format and NIST SP 800-53 control parameters, added a section on SCRM, included EO 13800 and NIST Cybersecurity Framework	Biennial update.	Throughout

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Revision 7 - September 21, 2022		
1	Salamon/ LeVan/Dean/ Klemens	Revisions included: • Updated to NIST SP 800-53, Revision 5 controls and GSA parameters. • Updated style, format, guidance, and content.	Align to current NIST guidance and GSA parameters. New or substantively changes controls from Revision 5 are: IA-1, IA-2(2), IA-2(5), IA-2(8), IA-4, IA-4(4), IA-5, IA-5(1), IA-5(6), IA-8(4), IA-11, IA-12, IA-12(2), IA-12(3), IA-12(4), IA-12(5)	Throughout

Approval

IT Security Procedural Guide: Identification and Authentication (IA), CIO-IT Security-01-01, Revision 7, is hereby approved for distribution.

DocuSigned by:

Bo Berlas

FD717926161544F...

Bo Berlas
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), ICAM Shared Services Division (ISI) at icam-portfolio@gsa.gov

Table of Contents

Notes:

- Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section or an appendix). Hyperlinks will be provided for external sources unless the hyperlink is to a web page or document listed in Appendix C.
- It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.
- Two acronyms for Identification and Authentication, (I&A) and (IA), are used throughout this guide. IA is used when referring to NIST SP 800-53 security controls or in relation to those controls. I&A is used when referring to processes, features, or mechanisms used to implement user identification and authentication.

1 Introduction

1.1 Overview

Identification and authentication (I&A) are critical to securing General Service Administration (GSA) systems and their components.

- Account management deals with the creation and management of system accounts.
- Identification focuses on assignment and management of accounts to users and devices.
- Authentication focuses on verifying the claimed account or identity of users and devices before providing any type of access to an information system.

An effective approach for identifying and authenticating users and devices is often the first line of defense for protecting information technology (IT) assets and data. It provides a process for the assignment and management of user and device accounts as well as establishing strong authentication policies to protect GSA systems from unauthorized access and use.

The mechanisms associated with I&A, when effectively applied, ensure that users or devices accessing or connecting to GSA's IT resources are indeed who they represent themselves to be.

Account mechanisms are when a user or device is provided a unique name in a system. The most commonly used account mechanisms are:

- Usernames, or
- System unique identifiers that a user enters or device sends/provides.

GSA requires unique accounts.

The most commonly known authentication mechanisms are usernames coupled with passwords.

- The username is the account reference.
- The password is the authentication for that account.

Passwords alone as a single authentication factor are weak and easier to compromise. Passwords are persistent shared secrets. GSA requires strong authentication mechanisms for users and devices including:

- Multi-factor authentication (MFA) for users.
- Strong authentication for devices, application programming interfaces (APIs), service accounts and similar items.

Some multi-factor authentication options for users are covered in Section 4. The use of MFA and to a lesser extent, unique account names help to ensure the confidentiality of GSA information and the integrity of IT resources.

Every GSA system must follow the practices described in this guide. Any deviations from the security requirements established in GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy," must be coordinated by the appropriate Information Systems Security Officer (ISSO) through the appropriate Information Systems Security Manager (ISSM) and approved by the Authorizing Official (AO). Any deviations, exceptions, or other conditions not following GSA policies and standards must be submitted using the Security Deviation Request Google Form.

Executive Order (EO) 13800, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," requires all agencies to use "The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology (NIST) or any successor document to manage the agency's cybersecurity risk." This NIST document is commonly referred to as the Cybersecurity Framework (CSF). GSA uses NIST Special Publication (SP) 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," commonly referred to as the RMF, as its foundation for managing risk, including the implementation of NIST SP 800-53 IA controls. Further information on how IA controls relate to the CSF is provided in Appendix A.

1.2 Digital Identity Acceptance Statement

Per CIO 2100.1, all information systems allowing authentication of users for the purpose of conducting government business electronically (accessed via the Internet or via other external non-agency controlled networks, such as partner virtual private network [VPN]) complete a Digital Identity Acceptance Statement in accordance with NIST Special Publication (SP) 800-63-3.

A GSA Digital Identity Acceptance Statement template is available on the IT Security Forms and Aids InSite webpage. The template assists in determining a system's Identity Assurance Level (IAL), Authentication Assurance Level (AAL), and optionally, a Federation Assurance Level (FAL), based on guidance in the NIST SP 800-63 series on digital identities.

1.3 Organizational Access

Access to organizational information systems is defined as either local or network.

- Local access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network.
- Network access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection.

DocuSign Envelope ID: 15855DB6-50B5-4FA8-94EA-93EC0093760A

- Remote access is a type of network access which involves communication through an external network (e.g., the Internet).
- Internal networks include local area networks, wide area networks, and virtual private networks that are under the control of the organization.
- For a virtual private network (VPN), the VPN is considered an internal network if the organization establishes the VPN connection between organization-controlled endpoints in a manner that does not require the organization to depend on any external networks across which the VPN transits to protect the confidentiality and integrity of information transmitted.

1.4 Purpose

The purpose of this guide is to provide guidance for the IA controls identified in NIST SP 800-53 and IA requirements specified in CIO Order 2100.1. It provides specific procedures and processes systems are to follow for implementing NIST SP 800-53 IA controls.

1.5 Scope

This procedural guide is for:

- GSA Federal employees and contractors with significant security responsibilities;
- Other information technology personnel involved in implementing IA controls, features, and mechanisms; and
- All GSA information systems.

Per CIO 2100.1, a GSA information system is an information system:

- used or operated by GSA; or
- used or operated on behalf of GSA by a contractor of GSA or by another organization.

1.6 Policy

Appendix B contains the CIO 2100.1 policy statements regarding identification and authentication for GSA systems. GSA's Enterprise Identity, Credential, and Access Management (ICAM) Policy, including ICAM governance requirements, are identified in CIO 2183.1.

1.7 References

Appendix C provides links to references used throughout this guide.

2 Roles and Responsibilities

There are many roles associated with implementing effective IA policies and procedures. System owners for each information system are responsible for ensuring that I&A processes exist for their specific systems and that the appropriate personnel have been assigned I&A activities/tasks to satisfy the NIST IA control requirements. Appendix D provides a listing of roles and responsibilities related to implementing, administering, managing, monitoring, I&A for systems at GSA.

3 GSA Implementation Guidance for IA Controls

The GSA-defined parameter settings included in the control requirements are in blue, italicized text and offset by brackets in the control text.

The GSA implementation guidance stated for each control applies to personnel and/or the systems operated on behalf of GSA. Any additional instructions or requirements for contractor systems are included in the "Additional Contractor System Considerations" portion of each control section.

Table 3-1 identifies the designation of IA controls as Common, Hybrid, or System-Specific Controls for both Federal and Contractor systems.

- *Common* controls are provided by GSA at the enterprise level or by one of GSA's Major Information Systems (e.g., General Support System),
- *System specific* controls are implemented at the system level, and
- *Hybrid* controls have shared responsibilities.

CIO-IT Security-18-90: Information Security Program Plan (ISPP), describes the GSA enterprise-wide common and hybrid controls and outlines the responsible parties for implementing them.

Note: Until the ISPP is updated to NIST SP 800-53, Revision 5, contact ispcompliance@gsa.gov for guidance if there is a discrepancy between this guide and the ISPP.

Table 3-1: Designation of IA Controls

System Type	Federal	Contractor
Common	IA-1	
Hybrid	IA-2, IA-2(1), IA-2(2), IA-2(8), IA-2(12), IA-4, IA-4(4), IA-5, IA-5(1), IA-5(2), IA-5(6), IA-5(7), IA-6, IA-7, IA-8, IA-8(1), IA-8(2), IA-8(4), IA-11, IA-12, IA-12(2), IA-12(3), IA-12(5)	IA-1
System-Specific	IA-2(5), IA-3, IA-12(4)	IA-2, IA-2(1), IA-2(2), IA-2(5), IA-2(8), IA-2(12), IA-3, IA-4, IA-4(4), IA-5, IA-5(1), IA-5(2), IA-5(6), IA-5(7), IA-6, IA-7, IA-8, IA-8(1), IA-8(2), IA-8(4), IA-11, IA-12, IA-12(2), IA-12(3), IA-12(4), IA-12(5)

Table 3-2 identifies IA control applicability at the FIPS 199 Low, Moderate, and High levels, and for GSA's Lightweight (LATO) and Moderate Impact Software-as-a Service (MiSaaS) assessment and authorization (A&A) processes.

Table 3-2: IA Control Applicability

FIPS 199 Level/A&A Process	Applicable Controls
Low	IA-1, IA-2, IA-2(1), IA-2(2), IA-2(8), IA-2(12), IA-4, IA-5, IA-5(1), IA-6, IA-7, IA-8, IA-8(1), IA-8(2), IA-8(4), IA-11
Moderate	IA-1, IA-2, IA-2(1), IA-2(2), IA-2(8), IA-2(12), IA-3, IA-4, IA-4(4), IA-5, IA-5(1), IA-5(2), IA-5(6), IA-5(7)**, IA-6, IA-7, IA-8, IA-8(1), IA-8(2), IA-8(4), IA-11, IA-12, IA-12(2), IA-12(3), IA-12(5)
High	IA-1, IA-2, IA-2(1), IA-2(2), IA-2(5), IA-2(8), IA-2(12), IA-3, IA-4, IA-4(4), IA-5, IA-5(1), IA-5(2), IA-5(6), IA-5(7)**, IA-6, IA-7, IA-8, IA-8(1), IA-8(2), IA-8(4), IA-11, IA-12, IA-12(2), IA-12(3), A-12(4), IA-12(5)
LATO	IA-2, IA-2(1), IA-2(2)
MiSaaS	IA-2, IA-2(1), IA-2(2), IA-2(12), IA-5, IA-5(7)

**-control is applicable at the level listed per GSA OCISO Tailored Moderate Baseline

Table 3-3 identifies GSA IA control applicability based on users and devices.

Table 3-3: IA User and Device IA Control Matrix

Type	Applicable Controls	Example
User: Organizational	IA-2, IA-4, IA-5, IA-6, IA-7, IA-11	Organizational users for GSA systems are employees, contractors, and affiliated personnel. Organizational users include: • GSA organizational employees, or • individuals who GSA the organization deems to have the equivalent status of employees. Individuals with equivalent status include individuals provided gsa.gov accounts or provided routine, recurring access to GSA enterprise IT systems. Examples include contractors, guest researchers, detailees from other federal agencies, interns and similar.
Devices	IA-3, IA-4, IA-5, IA-7	A device can include virtual or physical workstations, servers, mobile, external hard drives, etc. Devices might also include “non-person” entities (NPEs) such as robot process automation (RPA), machine learning, artificial intelligence, etc.
User: Non-organizational	IA-4, IA-5, IA-6, IA-7, IA-8, IA-11, IA-12	A non-organizational user for GSA systems includes partners, other federal agency users, vendors, buyers or public consumers, or similar, who GSA does not directly manage or is not affiliated with GSA under the organizational user scope.

3.1 IA-1 Policy and Procedures

Control:

a. Develop, document, and disseminate to [*personnel with IT security responsibilities as defined in GSA CIO Order 2100.1*]:
   1. [*Organization-level*] identification and authentication policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and

c. Review and update the current identification and authentication:
   1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

Common Control Implementation:

The GSA identification and authentication policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding identification and authentication for GSA systems. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency website.

Identification and authentication procedures are documented in CIO-IT Security-01-01, "IT Security Procedural Guide: Identification and Authentication (IA)" [this guide]. The procedures facilitate the implementation of policies regarding identification and authentication and associated IA controls. The guide is disseminated GSA-wide via GSA's InSite centralized agency website.

Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.

The GSA OCISO is responsible for reviewing and updating CIO 2100.1 annually and CIO-IT Security-01-01 [this guide] every three years and following changes to Federal or GSA policies, requirements, or guidance which necessitate an update to the policy and/or this guide.

Federal System System-Specific Expectation:
None, IA-1 is a common control. However, GSA Service and Staff Offices (SSOs) or System Owners may augment the identification and authentication policies and procedures included in 2100.1 and CIO-IT Security-01-01 to address additional organizational or system-specific identification and authentication requirements. Any such policies and procedures must establish timeframes for updating them.

Additional Contractor System Considerations: Vendors/contractors may defer to the GSA policy and guide or implement their own identification and authentication policies and procedures which comply with GSA's requirements with the approval of the AO.

3.2 IA-2 Identification and Authentication (Organizational Users)

Control: Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

Control Enhancements:

(1) Identification and Authentication (Organizational Users) | Multifactor Authentication to Privileged Accounts. Implement multi-factor authentication for access to privileged accounts.

(2) Identification and Authentication (Organizational Users) | Multifactor Authentication to Non-Privileged Accounts. Implement multi-factor authentication for access to non-privileged accounts.

(5) Identification and Authentication (Organizational Users) | Individual Authentication With Group Authentication. When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

(8) Identification and Authentication (Organizational Users) | Access to Accounts — Replay Resistant. Implement replay-resistant authentication mechanisms for access to [*privileged and non-privileged accounts*].

(12) Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials . Accept and electronically verify Personal Identity Verification-compliant credentials.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

The focus of IA-2 is to implement unique identification and authentication of organizational users to the level of an individual/process. This control is not concerned with privileges but is concerned with binding the identity (user or process acting on behalf of user) to the identification/authentication process. This control is applicable to all components of a system.

Organizational users include:

- GSA employees, or
- individuals who GSA deems to have the equivalent status of employees.

Individuals with equivalent status include individuals provided gsa.gov accounts or provided routine, recurring access to IT systems. Examples include contractors, guest researchers, detailees from other federal agencies, interns and similar.

Examples of how the authentication of user identities is accomplished include:

- Integrate with GSA approved centralized authentication services using Security Assertion Markup Language (SAML 2.0) or OpenID Connect.
- The centralized authentication services will manage the multi-factor authentication options available to the users to allow for users to have accessible and secure options suited for their affiliation, and interaction with the system.

Multi-factor authentication options made available by centralized authentication services, or by the system directly, are dependent on the user. For organizational users (@gsa.gov), government-wide policies may take precedence based on GSA's enterprise risk management decisions. New or modernizing applications must have their authentication options evaluated by the ICAM Portfolio, as identified in CIO 2183.1

For organizational users (@gsa.gov), multi-factor authentications made available by the centralized authentication systems, or by the system directly, should only include methods in Table 3-4.

Table 3-4: Applicable MFA Methods

Authentication Method	Example	Target Date
Personal Identity Verification (PIV), or similar hardware based PKI token (e.g., GSA short-name account tokens for privileged accounts)	PIV, CAC, or GSA's short name account tokens provide for verifier-impersonation resistance and phishing resistance.	***Go-to target*** • Plan to be implemented by end of FY 2024
WebAuthn/FIDO2	WebAuthn may provide both factors, or as a 2nd factor, to provide for verifier-impersonation resistance and phishing resistance.	***Go-to target*** • Plan to be implemented by end of FY 2024
Push based notifications as the 2nd factor	Push based notifications are verifier-compromise resistant. This is a better option for usability and security than one-time password options. However, verifier-impersonation resistance is a go-to target state.	***Sunsetting*** • Plan to be deprecated by end of FY 2024
Time-based One Time Passwords using a mobile application as the 2nd factor	Time-based One Time Passwords using a mobile application are a better option for usability and security than one-time passwords via email. However, verifier-impersonation resistance is a go-to target state.	***Sunsetting*** • Plan to be deprecated by end of FY 2024

Authentication Method	Example	Target Date
Time-based One Time Passwords via a managed email as the 2nd factor	Managed email includes gsa.gov email addresses which are managed by GSA services and protected	***Sunsetting*** • Plan to be deprecated by end of FY 2024

Accessibility and diversity shall be considered and incorporated for all systems and options for organizational users to use multi-factor authentication successfully.

In addition to identifying and authenticating organizational users at the application level (i.e., at logon), identification and authentication mechanisms are employed at other components of the information system (e.g., operating system, database, servers, when necessary, to uniquely identify and authenticate users.

The outcome of this control is that an effective process has been implemented in which users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in control AC-14, Permitted Actions without Identification or Authentication. Every function that is not mentioned in AC-14 must have an identification and authentication capability and must be addressed in the control discussion.

Unique identification of individuals in group accounts may need to be considered for detailed accountability of activity.

Inheritance: The requirements for IA-2 may be fully satisfied as a common control or partially satisfied as a hybrid control if IA processes for all individuals (e.g., employees, contractors, guest researchers, and other authorized individuals) and system/service accounts are provided by having an account created and managed in GSA's Active Directory infrastructure (GSA Enterprise Infrastructure Operations [EIO] system). The creation of the user accounts integrates with GSA enterprise processes including our PIV credentialing and background investigation processes and systems, and integrations with routine training systems for our requirements for security training, rules of behavior and similar.

Details on how IA is implemented in GSA's AD implementation is documented in the most current GSA EIO System Security and Privacy Plan (SSPP).

Authentication of users for enterprise web and mobile applications is achieved through the integration of these GSA applications with the GSA Enterprise SSO platform which leverages:

- The GSA (gsa.gov) employee and affiliated contractor user accounts created and managed in these enterprise directories (GSA Active Directory).
- Only the users and accounts created and managed by GSA will successfully authenticate.
- As GSA users leave GSA, the accounts are removed through our enterprise off-boarding processes and procedures.

If a system implements separate I&A at other component levels (i.e., not leveraging the I&A of GSA enterprise users (@gsa.gov) from GSA's enterprise implementation, then the I&A

mechanisms at the component levels (e.g., operating system, database, application) must also meet the IA controls required based on the system's FIPS 199 level.

Solutions that satisfy GSA's multifactor authentication requirements for organizational users (@gsa.gov) include:

- Integrate with GSA approved centralized authentication services using Security Assertion Markup Language (SAML 2.0) or OpenID Connect, or:
- Multi-factor authentication options made available by the system directly.

Accessibility and diversity shall be considered and incorporated for all systems and options for organizational users (@gsa.gov) to use multi-factor authentication successfully.

To promote efficiency, effectiveness, and centralized monitoring and management - integrations with the centralized authentication services are the preferred option for most GSA managed systems. A request for deviation or plan of action and milestones, timelines and budget estimates may be required for any systems not integrating with centralized authentication services. New or modernizing applications must have their authentication options evaluated by the ICAM Portfolio, as identified in CIO 2183.1

Multi-factor authentication options made available by the centralized authentication services are listed in Table 3-4.

Additional Contractor System Considerations*:* Contractor systems may not be able to integrate with GSA provided enterprise authentication services due to the cost recovery options available. Contractor systems not utilizing or able to utilize GSA I&A enterprise authentication services must comply with the control in accordance with the guidance above. Contractor systems must provide the system's I&A settings to GSA for review and approval by the AO and concurrence by the GSA CISO.

3.3 IA-3 Device Identification and Authentication

Control: Uniquely identify and authenticate [*GSA SSO or Contractor recommended and GSA CISO and AO approved specific and/or types of devices*] before establishing a [*local, remote, or network*] connection.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

The IA-3 control is the equivalent of IA-2, however IA-3 is focused on the unique I&A of devices or non-person entities, rather than individuals.

Control implementations must identify the specific devices or device types for which I&A is required before establishing connections to an information system; and the information system only establishes connections after it has verified the unique identity and the identity is authenticated for the defined devices.

The devices requiring unique I&A may be defined by type, by specific device, or by a combination of type and device as deemed appropriate. The information system typically uses either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for identification or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, etc.) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the FIPS 199 security categorization of the information system and the confidentiality of the information that is being accessed and protected.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.4 IA-4 Identifier Management

Control: Manage system identifiers by:

a. Receiving authorization from [*personnel with identifier assignment authorization as defined in GSA CIO Order 2100.1*] to assign an individual, group, role, service, or device identifier;
b. Selecting an identifier that identifies an individual, group, role, service, or device;
c. Assigning the identifier to the intended individual, group, role, service, or device; and
d. Preventing reuse of identifiers for [*GSA SSO or Contractor recommended and GSA CISO and AO approved time period*].

Control Enhancements:

(4) Identifier Management | Identify User Status. Manage individual identifiers by uniquely identifying each individual as [*a GSA employee, a GSA internal contractor, or other characteristic as determined by GSA SSO and approved by the GSA CISO and AO*].

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

This control addresses the authorization, creation, and management of user and device identifiers (accounts/names). Where IA-2 focused on uniquely identifying and authenticating users (and processes acting on the behalf of users), IA-4 focuses on the procedures and processes that have been established by the organization for managing identifiers for individuals, groups, roles, and devices. This control is associated with AC-2, Account Management, and serves an integral part in overall management and protection of user and device identifiers/accounts through the implementation of processes to support the requirements stated in the control objectives.

Successful implementation of this control will consist of the following processes/procedures:

- **Authorization to issue a user account from an appropriate organization official.** Approval by at least one supervisor must be received prior to an account being issued. The authorization process begins when a manager or supervisor submits an account request for a new GSA employee or contractor. This request is reviewed by an authorized GSA official who must sign off on the request in order for an account to be created and issued. In addition, GSA requires annual reviews of accounts for reauthorization. All user accounts must be reviewed annually by the System Owner, Program Manager, and/or ISSO to ensure active accounts are still required for authorized personnel.

- **Creation of unique names for each user or device account.** GSA uses several naming schemes in accordance with the account types and functions. Non-privileged user accounts (Long Name Accounts) use an individual’s full name as the identifier. Most commonly, users are assigned long name accounts for day-to-day business needs and have no administrative rights or permissions assigned to them. These accounts are most commonly used in naming our GSA enterprise active directory accounts. Privileged (administrative) user accounts (Short Name Accounts) are named to uniquely identify the individual and/or role they serve.

- **Verification of user identity prior to issuance of an account.** Employees and contractors must submit to a background investigation and employment suitability review, prior to being granted user accounts to access GSA networks and IT resources.

- **Issuing the account to the intended party.** GSA accounts are uniquely assigned and identifiable to individual employees and contractors. All service accounts should be assigned to an individual and those individuals made responsible, via position description or performance measures, for the management, use, and protection of the authentication credentials associated with a particular service account.

- **Defining within the security plan, explicitly or by reference, the time period of inactivity after which a user account is to be disabled.** GSA System Owners and ISSO’s must comply with GSA parameters provided for controls IA-4 and AC-2(2) and (3), and document within their respective system security plans the specific time period of inactivity whereby an account is to be disabled. Administrative accounts are required to be disabled immediately upon transfer or termination of the account holder.

- **Preventing the reuse of user accounts.** GSA requires non-administrative user accounts to be uniquely identifiable to an assigned user, and not to be reused or shared by any other party.

- **Disabling the account after the organization-defined time period of inactivity.** All GSA systems must disable or terminate user level accounts after 90 days of inactivity. Non-user level accounts (device, token, etc.) are deferred to the system (GSA SSO) for determination. The setting must be approved by the GSA Authorizing Official before implementation.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.5 IA-5 Authenticator Management

Control: Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;
b. Establishing initial authenticator content for any authenticators issued by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
e. Changing default authenticators prior to first use;
f. Changing or refreshing authenticators [*one time use passwords/PINs must expire in two minutes if based on a real-time clock*] or when [*compromised, recovered/forgotten, incident related events*] occur;
g. Protecting authenticator content from unauthorized disclosure and modification;
h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and
i. Changing authenticators for group or role accounts when membership to those accounts changes.

Control Enhancements:

(1) Authenticator Management | Password-Based Authentication. For password-based authentication:

(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [*within 12 months of the latest available version of the utilized bad and/or compromised password database checking service (e.g., haveibeenpwned.com)*]and when organizational passwords are suspected to have been compromised directly or indirectly;
(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);
(c) Transmit passwords only over cryptographically-protected channels;

(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;

(e) Require immediate selection of a new password upon account recovery;

(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;

(g) Employ automated tools to assist the user in selecting strong password authenticators; and

(h) Enforce the following composition and complexity rules: [

(1) Passwords for accounts used to access operating systems (workstations and servers) must:

(a) Contain a minimum of 16 characters;

(b) Have passwords changed when a password is compromised or forgotten; and

(c) Not have complexity requirements.

(2) *Passwords for system/other accounts (e.g., user, service, application) must:*

(a) Contain a minimum of 8 characters;

(b) Have passwords changed when a password is compromised or forgotten; and

(c) Require a combination of letters, numbers, and special characters if no password checking solution is used; or

(d) Have no complexity requirements, if a password checking solution to check a database of known bad passwords is used (e.g., checks for commonly used, expected, or compromised passwords; dictionary words; repetitive or sequential characters such as 'aaaaaaa,' '1234abcd,' '1qaz2wsx;' or context sensitive words such as the username or a derivative).

(3) *Passwords for all mobile devices such as GSA approved smartphones, iPads, and tablets must be a minimum of 6 characters. The six-character password requirement also applies to personal mobile devices accessing GSA data or systems.*]

(4) Authenticator Management | Public Key-Based Authentication.

(a) For public key-based authentication:

(1) Enforce authorized access to the corresponding private key; and

(2) Map the authenticated identity to the account of the individual or group; and

(b) When public key infrastructure (PKI) is used:

(1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and

(2) Implement a local cache of revocation data to support path discovery and validation.

(6) Authenticator Management | Protection of Authenticators. Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

(7) Authenticator Management | No Embedded Unencrypted Static Authenticators. Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

Initial Password Creation and Distribution:
A secure method for initial distribution of passwords and PINs should be documented in the system security plan and implemented for each IT resource. The administrator can create the account and an initial strong password (randomly chosen from a large space), provide it to the user, and instruct the user to use the password only for an initial login. The initial password should be set to expire at first use. The user must be instructed to select a proper password based upon GSA's password guidelines. For especially sensitive applications, consider providing initial authentication information over the telephone after verifying the individual's identity.

In addition to the requirements specified in the control parameters for IA-5 and its enhancements, the following password policies/restrictions apply.

Password Policies/Restrictions:

- All default passwords on network devices, databases, operating systems, etc. must be changed.
- Passwords (and PINs) must never be sent via e-mail, regular mail, or interoffice mail.
- Password distribution:
  - User IDs and passwords must never be distributed together.
  - User IDs and passwords must be distributed via separate channels when not performed in person.
  - Passwords used for authentication must not be transmitted in the clear.
- To protect passwords, web sites (internal and public) with logon functions, must implement TLS encryption with a FIPS 140-3/140-2[1] validated encryption module.

Password Administration:

- **Disable/change all default accounts and passwords.**
  Most operating systems and applications including databases install with default accounts and passwords, some of which have critical system privileges. Disabling and changing all default accounts and passwords will prevent most scripted attacks and will delay more advanced manual attacks on a system.
- **Disable user accounts as quickly as possible when the user is no longer authorized resource access.**
  Delete an account once files associated with an account have been reviewed and reassigned or removed.

[1] *NIST has issued FIPS 140-3, however FIPS 140-2 modules will be accepted through September 21, 2026. For additional information see NIST Cryptographic Module Validation Program (CMVP).*

- **Change passwords when a compromise is suspected.**
  An automated password system should allow the administrator to delete or replace a password, and it should have the capability to maintain a record of when a password was created or changed.
- **Reset passwords.**
  When resetting passwords, user identity must be verified. This can be done either in person or having the user answer questions for which the answers are only expected to be known by the user (i.e., not publicly available or easily attainable) that can be compared to the correct answers in the administrator's database. Passwords forgotten by their owner should be changed, not reissued.

Changing/Refreshing Passwords:
Users must be authenticated before resetting or distributing a password. Self-service password resets are commonly available in web based applications and identity management software. The function allows users who have forgotten passwords or inadvertently locked out their account to repair/reset it themselves without involvement of the help desk. The feature expedites problem resolution involving password resets but can also introduce new attack vectors that could result in system compromise if implemented insecurely.

GSA does not encourage the use of knowledge-based questions in self-service password reset functions. The use of such functions must adhere to the guidance in NIST SP 800-63A regarding the use of knowledge-based verification of identity.

Password Storage:
All passwords must be encrypted in storage. Passwords must not be stored in forms (i.e., Windows dialog boxes, web forms, etc.). Do not store passwords in clear text form (unencrypted). Password-only mechanisms, especially those that transmit the password in the clear can be monitored and captured. Encryption converts data into unintelligible code. This process causes data to be unreadable to anyone who does not have the key to decrypt it. The data will remain private and confidential, regardless of whether it is being transmitted or stored on a computer when encrypted. Those without authorization will be unable to decrypt the encrypted passwords.

When a password is typed, the IT resource must determine whether it is right. If the IT resource stores the passwords unencrypted, anyone with access to the IT resource storage or backup tapes can steal passwords. It is not necessary for the IT resource to know a password to verify if it is correct.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.6 IA-6 Authenticator Feedback

Control: Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

The focus of this control is to assure that passwords which are entered into information systems are not visually displayed in clear text during entry. Typically, authenticator feedback is obscured by displaying asterisks instead of the actual password. The control does not cover feedback regarding the success or failure of an authentication attempt (which is covered by SI-11); and does not cover machine to machine authentication (which is addressed in IA-5).

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.7 IA-7 Cryptographic Module Authentication

Control: Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

The focus of this control is to implement FIPS 140-3/140-2 validated encryption modules for authentication where encryption is required. Validated Cryptographic Modules can be found by on NIST’s Cryptographic Module Validation Program search webpage and selecting “Advanced” for Search Type, then selecting “140-3” or “140-2” as the Standard and “Active” as the Validation Status when searching.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.8 IA-8 Identification and Authentication (Non-Organizational Users)

Control: Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

Control Enhancements:

(1) Identification and Authentication (Non-Organizational Users) |Acceptance of PIV Credentials From Other Agencies. Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.

(2) Identification and Authentication (Non-Organizational Users) |Acceptance of External Party Credentials.

(a) Accept only external authenticators that are NIST-compliant; and

(b) Document and maintain a list of accepted external authenticators.

(4) Identification and Authentication (Non-Organizational Users) | Use of Defined Profiles. Conform to the following profiles for identity management [*requirements identified in GSA Order CIO 2183.1*].

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

In accordance with the Digital Identity Acceptance Statement, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy related information. Accordingly, a risk assessment is used in determining the authentication needs of a system with non-organizational users. Scalability, practicality, and security are simultaneously considered in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk to organizational operations, organizational assets, individuals, and other organizations. IA requirements for information system access by organizational users are described in IA-2.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.9 IA-11 Re-Authentication

Control: Require users to re-authenticate when [*Passwords are reset, privileged functions are executed, and/or periodic reauthentication time limits are met. Reauthentication times are predicated on NIST 800-63B Authenticator Assurance Levels (See Section 4). Specifically: (1) After 30 minutes of inactivity at all levels; (2) The following timeframes regardless of user activity a. Thirty (30) days for systems at AAL1; b. Twelve (12) hours for systems at AAL2 and AAL3*].

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

The focus of this control is to ensure users have to re-authenticate themselves under certain conditions and the AAL of the system based on the system's Digital Identity Acceptance Statement AAL level. Systems are required to have users re-authenticate when their password is reset, they execute a privileged function, or they are inactive for the timeframes listed in the parameter based on AAL level. Device lock which would also require re-authentication is covered under control AC-11.

***Additional Contractor System Considerations:** Vendors/contractors are required to comply with the control statements.*

3.10 IA-12 Identity Proofing

Control:

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;
b. Resolve user identities to a unique individual; and

c. Collect, validate, and verify identity evidence.

Control Enhancements:

(2) Identity Proofing | Identity Evidence. Require evidence of individual identification be presented to the registration authority.

(3) Identity Proofing | Identity Evidence Validation and Verification. Require that the presented identity evidence be validated and verified through [mechanism(s) that support the IAL level determined when completing the GSA Digital Identity Acceptance Statement].

(4) Identity Proofing | In-Person Validation and Verification. Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.

(5) Identity Proofing | Address Confirmation. Require that a [*notice of proofing (applicable to IAL2 and IAL3 systems) in accordance with NIST SP 800-63A, and the GSA Digital Identity Acceptance Statement for the application*] be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

The focus of this control is to ensure a user is who they say they are before issuing them credentials to access a system. The level of assurance of the evidence required to ascertain a user is uniquely who they say they are, is based on the IAL level determined in the Digital Identity Acceptance Statement. NIST SP 800-63A, Digital Identity Guidelines & Identity Proofing, lists acceptable evidence for identity proofing at the various IALs. For organizational users, users with gsa.gov accounts, they will have gone through GSA's onboarding process and been issued a PIV which satisfies identity proofing at IAL3 (the highest level). The requirements for IA-12 may be fully satisfied as a common control if users are managed in GSA's Active Directory [AD] infrastructure (GSA Enterprise Infrastructure Operations [EIO] system). The verification of user identities is provided by GSA enterprise processes including PIV credentialing and background investigation processes. Details are documented in the most current GSA EIO System Security and Privacy Plan (SSPP).

Systems not integrating with GSA's AD infrastructure and/or identity verification processes must have processes in place to support the required evidence per IAL level for users. The identity proofing process must be documented in the system's SSPP.

Additional Contractor System Considerations: *Vendors/contractors are required to comply with the control statements.*

Appendix A: CSF Categories/Subcategories

The CSF focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The core of the CSF consists of five concurrent and continuous Functions—Identify (ID), Protect (PR), Detect (DE), Respond (RS), Recover (RC). The CSF complements, and does not replace, an organization's risk management process and cybersecurity program. GSA uses NIST's Risk Management Framework (RMF) from NIST SP 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy." Table A-1 lists the Categories and Subcategories from the CSF that are identified as related to the implementation of policies, procedures, and processes regarding the NIST SP 800-53 IA control family controls documented in this guide. GSA CIO Order 2100.1 and this procedural guide provide GSA's policies and procedural guidance regarding identification and authentication to GSA systems and implementing IA controls.

Table A-5: CSF Categories/Subcategories and the IA Family

CSF Category/Subcategory Identifier	Definition/Description
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated *(CIO Order 2100.1 and Appendix C of this guide)* **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed *(CIO 2100.1 and throughout this guide)*
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes *(IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-11, IA-12)* **PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions *(IA-1, IA-2, IA-4, IA-5, IA-8, IA-12)* **PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) *(IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-11)*

Appendix B: GSA CIO Order 2100.1 Policy Statements on Access Control

CIO 2100.1 contains the following policy statements regarding identification and authentication.

CIO 2100.1 Chapter 4, Policy for Protect Function

1. <u>Identity Management, Authentication and Access Control.</u>

b. All users issued GFE are required to log into the workstation using a GSA issued PIV credential. The following groups of users are exempt from this requirement:

(1) Federal employees on detail to GSA issued a PIV from their assigned Agency.
(2) Employees or contractors expected to be employed for less than 180 days and not issued a PIV.
(3) Any person with a disability prohibiting the use of a PIV card and laptop.
(4) Any user with a PIV that is lost, forgotten at home, or damaged in any way, may contact the IT Service Desk to request a temporary exception to the above requirement, not to exceed 45 days.

yy. All GSA systems must incorporate a proper user identification and authentication methodology. Refer to the GSA CIO-IT Security-01-01 for additional details

zz. User IDs shall be unique to each authorized user.

aaa. Authentication schemes for all systems and users must utilize MFA using two or more types of authentication factors. GSA systems with non-privileged users may integrate with GSA approved centralized authentication services using Security Assertion Markup Language (SAML 2.0) or OpenID Connect. The centralized authentication services will manage the multi-factor authentication options available to the users to allow for users to have accessible and secure options suited for their affiliation and interaction with the system. Multi-factor authentication options made available shall prefer smartcard based public key infrastructure and webauthn options for GSA non-privileged users. Multi-factor authentication options made available to GSA business or public users can include one-time passwords delivered via a mobile app or push notifications but shall offer choices for webauthn where feasible.

ddd. An authentication scheme using passwords as a credential must implement the following password policy requirements:

(1) Passwords for accounts used to access operating systems (workstations and servers) must:

(a) Contain a minimum of 16 characters;
(b) Have passwords changed when a password is compromised or forgotten; and
(c) Not have complexity requirements.

(2) Passwords for system/other accounts (e.g., user, service, application) must:

(a) Contain a minimum of 8 characters;
(b) Have passwords changed when a password is compromised or forgotten; and
(c) Require a combination of letters, numbers, and special characters if no password checking solution is used; or
(d) Have no complexity requirements, if a password checking solution to check a database of known bad passwords is used (e.g., checks for commonly used, expected, or compromised passwords; dictionary words; repetitive or sequential characters such as 'aaaaaaaa,' '1234abcd,' '1qaz2wsx;' or context sensitive words such as the username or a derivative).

(3) Passwords for all mobile devices such as GSA approved smartphones, iPads, and tablets must be a minimum of 6 characters. The six-character password requirement also applies to personal mobile devices accessing GSA data or systems.

(4) Passwords must not be stored in forms (i.e., Windows dialog boxes, web forms, etc.).

(5) All default passwords on network devices, databases, operating systems, installed software, etc. must be changed.

(6) Password distribution:

(a) Passwords must never be distributed via regular mail or interoffice mail.
(b) User IDs and passwords must never be distributed together.
(c) User IDs and passwords must be distributed via separate emails or channels (e.g., email, text, telephone).
(d) Passwords used for authentication (other than default or one time use passwords) must not be transmitted in the clear.

(7) Users must be authenticated before resetting or distributing a password.

(8) One time use passwords must expire in two minutes if based on a real-time clock.

(10) Password managers are permitted as long as they are listed on the GSA IT Standards List with a Status of Approved or Exception.

ccc. E-commerce and publicly accessible systems must incorporate identification and authentication mechanisms commensurate with their security risks and business needs and may differ from the security requirements set forth by this policy. In such cases the identification and authentication mechanisms must be approved by the AO in writing and concurred by the OCISO.

3. <u>Data Security.</u>

e. Web sites (internal and public) with logon functions, must implement Transport Layer Security (TLS) encryption with a FIPS 140-3/140-2 validated encryption module. SSL/TLS implementation must be IAW GSA CIO-IT Security-14-69: SSL/TLS Implementation Guide.

Appendix C: References

Federal Laws, Standards, Regulations, and Publications:

- EO 13800, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"
- FIPS PUB 140-3, "Security Requirements for Cryptographic Modules"
- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems"
- FIPS PUB 201-3, "Personal Identity Verification (PIV) of Federal Employees and Contractors"
- Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors"
- NIST CSF, "Framework for Improving Critical Infrastructure Cybersecurity"
- NIST SP 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy"
- NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations"
- NIST SP 800-63-3, "Digital Identity Guidelines"
- NIST SP 800-63A, "Digital Identity Guidelines: Enrollment and Identity Proofing"
- NIST SP 800-63B, "Digital Identity Guidelines: Authentication and Lifecycle Management"
- NIST SP 800-63C, "Digital Identity Guidelines: Federation and Assertions"
- OMB Circular A-130, "Managing Information as a Strategic Resource"

GSA Policies, Procedures, Guidance:

The GSA policies listed below are available on the GSA.gov Directives Library page.

- GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy"
- GSA Order CIO 2183.1, "Enterprise Identity, Credential, and Access Management (ICAM) Policy"

The GSA CIO-IT Security Procedural Guides listed below are available on the GSA.gov IT Security Procedural Guides page with the exception of CIO-IT Security-18-90 which is restricted. It is available on the internal GSA InSite IT Security Procedural Guides page.

- CIO-IT Security-06-30, "Managing Enterprise Cybersecurity Risk"
- CIO-IT Security-09-48, "Security and Privacy Requirements for IT Acquisition Efforts"
- CIO-IT Security-14-69, "SSL/TLS Implementation"
- CIO-IT Security-18-88, "Moderate Impact Software as a Service (MiSaaS) Security Authorization Process"
- CIO-IT Security-18-90, "Information Security Program Plan (ISPP)"

Appendix D: Roles and Responsibilities

The roles and responsibilities provided in this appendix have been extracted or paraphrased from CIO 2100.1 or summarized from GSA and Federal guidance. Complete roles and responsibilities for agency management officials and roles with significant IT Security responsibilities are defined in GSA CIO Order 2100.1.

Authorizing Official (AO)

Responsibilities include the following:

- Ensuring that GSA information systems under their purview have implemented the required IA controls in accordance with GSA and Federal policies and requirements.
- Identifying the level of acceptable risk for an information system and determining whether an acceptable level of risk has been obtained, including risks associated with IA controls.
- Ensuring all information systems, applications, or sets of common controls under their purview have a current Authorization to Operate (ATO) issued per GSA CIO-IT Security-06-30.
- Ensuring a plan of action and milestones (POA&M) entry is developed and managed to address any IA controls that are not fully implemented.

Information System Security Manager (ISSM)

Responsibilities include the following:

- Assisting ISSOs, as necessary, to ensure NIST SP 800-53 IA controls are in place and operating as intended.
- Verifying systems under their purview have appropriately addressed NIST SP 800-53 IA controls.
- Coordinating with the AO, System Owner, ISSOs, and OCISO Directors, as necessary, regarding IA control implementation and compliance with NIST and GSA requirements.
- Working with the ISSO and System Owner to develop and manage POA&Ms regarding IA controls that are not fully implemented for their respective systems per GSA CIO-IT Security-09-44.

Information System Security Officer (ISSO)

Responsibilities include the following:

- Ensuring necessary IA controls are in place and operating as intended.
- Coordinating with ISSMs and System Owners, as necessary, regarding IA control implementation and compliance with NIST and GSA requirements.

- Working with the System Owner and ISSM to develop and manage POA&Ms regarding IA controls that are not fully implemented for their respective systems per GSA CIO-IT Security-09-44.
- Ensuring the user identification and authentication scheme used in systems under their purview are administered as intended, including reviewing system role assignments to validate compliance with principles of least privilege.
- Assisting System Owners and Data Owners in verifying user accounts are only issued when authorized, verified annually, and terminated when no longer needed.

System Owner

Responsibilities include the following:

- Ensuring necessary NIST SP 800-53 IA controls are in place and operating as intended.
- Coordinating with ISSOs and ISSMs, as necessary, regarding IA control implementation and compliance with NIST and GSA requirements.
- Working with ISSOs and ISSMs to develop and manage POA&Ms regarding NIST SP 800-53 IA controls that are not fully implemented for their respective systems per GSA CIO-IT Security-09-44.
- Obtaining the resources necessary to securely implement and manage IA controls for their respective systems.
- Conducting annual reviews and validation of system users' accounts to ensure the continued need for access to a system and verify users' authorizations (rights/privileges).
- Working with the Data Owner, granting access to the information system based on a valid need-to-know/need-to-share that is determined during the account authorization process and the intended system usage.

Data Owner/Functional Business Line Manager/Custodian

Responsibilities include the following:

- Coordinating with IT security personnel including the ISSM and ISSO and System Owners to ensure implementation of IA control requirements, as necessary.
- Working with the System Owner, with assistance from the ISSO, to ensure system access is restricted to authorized users that have completed required background investigations, are familiar with internal security practices, and have completed requisite security awareness training programs (e.g., the annual IT Security and Privacy Awareness course).
- Reviewing access authorization listings and determining whether they remain appropriate at least annually.
- Ensuring information systems that allow authentication of users for the purpose of conducting Government business electronically complete a Digital Identity Acceptance Statement for digital transactions resulting in an assurance level classification IAW NIST SP 800-63-3, Digital Identity Guidelines

Authorized User of IT Resources

Responsibilities include the following:

- Ensuring that adequate protection is maintained on their workstation, including not sharing passwords with any other person and logging out, locking, or enabling a password protected screen saver, and removing their PIV card before leaving their workstation.
- Utilizing assigned privileged access rights (e.g., administrator, power user, database administrator, web site administrator, etc.) to a computer based on need-to use (i.e., using accounts with those privileges only when the privileges are required to complete an action).

System/Network Administrator

Responsibilities include the following:

- Ensuring the appropriate security requirements are implemented consistent with GSA IT security policies and hardening guidelines.
- Utilizing privileged access rights (e.g., “administrator,” “root,” etc.) to a computer based on a need-to-use basis (i.e., using accounts with those privileges only when the privileges are required to complete an action).
- Ensuring system/network administrators have separate administrator and user accounts, if applicable (e.g., Microsoft Windows accounts). A normal user account should be used unless administrator rights are required to perform a job function.
- Utilizing GSA provided MFA to ensure strong authentication.

Supervisor

Responsibilities include the following:

- Conducting annual review and validation of staff user accounts to ensure the continued need for access to a system.
- Conducting annual reviews of staff training records to ensure annual IT Security and Privacy Awareness Training, and application specific training has been completed for all users. The records shall be forwarded to ISSOs/system owners as part of the annual recertification efforts.
- Coordinating and arranging system access requests for all new or transferring employees and verifying an individual’s need to know (authorization).
- Coordinating and arranging system access termination for all terminating or transferring personnel.
- Coordinating and arranging system access modifications for personnel.

Appendix E: Definitions

All terms are consistent with the definitions from NIST's Glossary webpage. Definitions marked with an * are defined as listed for the purposes of this guide (i.e., not from the NIST webpage).

Accountability
The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

Adequate Security
Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Assurance
Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass.

Authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authenticator
The means used to confirm the identity of a user, process, or device (e.g., user password or token).

Authenticity
The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, message, or message originator. See authentication.

Authorization
Access privileges granted to a user, program, or process or the act of granting those privileges.

Confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Encryption
The process of changing plaintext into ciphertext using a cryptographic algorithm and key.

Identity
The set of physical and behavioral characteristics by which an individual is uniquely recognizable. Note: This also encompasses non-person entities (NPEs).

Identification
The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.

Identifier
Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers. Note: This also encompasses non-person entities (NPEs).

Integrity
Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Multifactor Authentication (MFA)
Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

Network
A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Network Access
Access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

Organization
An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).

Organizational User
An organizational employee or an individual whom the organization deems to have equivalent status of an employee, including a contractor, guest researcher, or individual detailed from another organization. Policies and procedures for granting the equivalent status of employees to individuals may include need-to-know, relationship to the organization, and citizenship.

Password*
A type of shared secret authenticator comprised of a character string intended to be memorized or stored by a user, permitting the user to demonstrate something they know as part of an authentication process. For devices and other non-person entities, a shared secret character string stored and passed to the receiving system.

Phishing-Resistant
See Verifier-Impersonation Resistant

DocuSign Envelope ID: 15855DB6-50B5-4FA8-94EA-93EC0093760A

Privileged Account
A system account with the authorizations of a privileged user.

Privileged User
A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Remote Access
Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).

Security Control Enhancements
Statement of security capability to: (i) build in additional, but related, functionality to a basic security control; and/or (ii) increase the strength of a basic control.

Validation*
The process of demonstrating that the system under consideration meets in all respects the specification of that system.

Verification
Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome).

Verifier-Compromise Resistant*
Authentication protocols that do not require the application (verifier) to persistently store secrets that could be used in the authentication process. For example, most one-time-password implementations require a secret to be shared between the application and the one time password generator. A user experience may include: scanning a QR code (which has the secret) to register the one-time-password app for the application. Verifier-compromise resistance is considered stronger than one-time-passwords; and include use of "push" notification protocols.

Verifier-Impersonation Resistant*
Verifier impersonation attacks, sometimes referred to as "phishing attacks," are attempts by fraudulent websites (i.e., systems, applications) to fool a user into authenticating to an impostor website (i.e., systems, applications). Authentication methods resistant to verifier-impersonation attacks are also referred to as "strongly man-in-the-middle resistant." Verifier-impersonation resistant authentication involves using a cryptographic challenge-response that is linked to the user authentication factor and the website (i.e., systems, applications) to prevent an imposter website from capturing and replaying the authentication factor. Verifier-impersonation resistance is implemented in modern implementations for web and mobile applications by having at least one factor that performs: mutual TLS (mTLS) based on asymmetric public-key infrastructure, or WebAuthn protocols using public-private keys.